The Evolution of TWIC

Coast Guard and TSA have teamed up to implement a common biometric identification card for use in the maritime industry.

by LCDR Jonathan Maiorine
Chief, Standards Branch, U.S. Coast Guard Office of Port and Facility Activities

In response to the Maritime Transportation Security Act (MTSA) of 2002, the Coast Guard has teamed up with the Transportation Security Administration (TSA) to work toward achieving one of the United States' most challenging security goals: develop, test, and implement a biometric transportation security card for an estimated one million U. S. maritime transportation workers, including all credentialed merchant mariners. While the requirement to issue a uniform identification credential for use across the entire maritime industry represented a significant task, the MTSA mandate to incorporate a biometric was immediately recognized as one of the most demanding aspects of the project for the Coast Guard.

Fortunately, when the Coast Guard joined the project in November 2004, TSA was actively engaged in researching and developing a Transportation Worker Identification Credential (TWIC) in response to the MTSA and the Aviation Transportation Security Act of 2001 (ATSA). The ATSA is aimed at strengthening airport access control points through the implementation of a secure credential. While the ATSA does not require the use of biometrics, language in the act does mandate that the use of biometrics be considered as a means of identifying airport employees.

TSA had already completed a technology review and had begun testing a biometric prototype TWIC when the Coast Guard offered to serve as a subject matter expert in implementing the TWIC first in the maritime mode. The ATSA required consideration of the use of biometrics in the airline industry, and the MTSA mandated the use of biometrics in the maritime mode. Therefore, teaming up Coast Guard and TSA in a joint rule-making project to implement a common biometric identification card in the maritime mode was a move in the right direction. It was also in step with Department of Homeland Security (DHS) policy advocating sharing of resources, technology, and information between agencies to enhance homeland security.

The Biometrics Challenge

On its Website, TSA defines biometrics as "automated methods of recognizing a person based on physiological or behavioral characteristics that are unique to an individual." Many people are familiar with the use of deoxyribonucleic acid (DNA) and fingerprints in law enforcement and forensic activities, but they may not realize that both fall into the broad category that is biometrics. While television and movies might project that the use of biometrics is common and fully established, in actuality, its use as a means of personal identity verification remains somewhat of an emerging industry.

Directed for use by such a large segment of the population, the TWIC will be the first of its kind in the United States. To establish a simple means by which a port worker can reliably identify himself or herself involves the use of a complex system. Such a system, however, will benefit national security, facility owners, and port employees by limiting unescorted access to secure areas and sensitive infrastructure to those individuals with a legitimate need and who also pass a security threat assessment.

Scope

Preliminary estimates indicate approximately one million workers will be enrolled in the TWIC maritime program. The MTSA-regulated industry, consisting of 3,500 facilities, 10,000 vessels, and 60 outer-continental shelf platforms, will be required to implement systems and policies to support the card and have their security plan updates approved by the Coast Guard.

The TWIC population, with regard to who is required to hold the credential, is mandated by the law itself, and this somewhat tangible data served as a cornerstone during the development of enrollment, card issuance, and data management plans. The development of the facility, vessel, and platform operational regulations, however, poses a unique challenge due to the broad range of operations, geographic locations, and varying numbers of workers requiring unescorted access to secure areas.

Sample Transportation Worker Identification Credential (TWIC), front and back.

The law clearly mandated that a biometric card will be issued. Developing the "how to use it" regulations is the tough part. Impacted vessels vary from 30-foot passenger sport fishing boats to 800-foot cargo ships, and facilities range from small riverfront fueling docks to multi-acre container terminals, refineries, and chemical plants. The challenge is to propose useful and workable regulations and an implementation schedule to support the TWIC's enhanced security capabilities without overburdening industry. Currently, TWIC regulatory development teams are exploring the different card authentication tools available to provide maximum flexibility for regulated entities.

Impact

What are the security problems currently faced by the various modes of the U.S. transportation system and supply chain that TWIC aims to solve? According to Mr. John Schwartz, assistant director of maritime and surface credentialing (MSC) programs at TSA, these are: "the inability to positively identify individuals entering secure areas of the transportation system; the inability to assess the threat posed by individuals due to a lack of background information, or the lack of uniformly determined background information; and the inability to protect current credentials against fraud." He added, "the TWIC will positively tie the person to the credential, to the threat assessment."

In storing a transportation worker's physical biometric, fingerprints, the TWIC will enable a one to one match of the cardholder to the card itself with the assistance of an electronic reader. Through development and publishing of the standard to which readers must comply, TSA encouraged competition among private sector vendors and intends for customers to benefit from the use of off-the-shelf technology.

The issue of interoperability itself has challenged the biometrics industry as a whole. Due to the fact that manufacturers can use a unique and proprietary algorithm to convert fingerprint images to templates for storage within the TWIC, a card reader manufactured by a different company may not be able to read the information stored by another. According to an article by Mr. Thad Rueter of *Card Technology* magazine, "to overcome that hurdle, vendors have worked to develop interoperable templates, which are currently being tested by the National Institute of Standards and Technology."

The TWIC is designed to be more secure than many other forms of identification, in part due to the storage of encrypted information on a contactless chip. Other information, including the cardholder's name, photo, and biometric, will be stored within the card's integrated circuit chip. Another feature of the TWIC system is the ability to cross reference a TSA-managed database for expired or revoked cards and compare names to threat-intelligence databases or watch lists.

Understandably, privacy and collection of personal information concerns have been voiced by personal privacy advocates such as the Electronic Privacy Information Center (EPIC), who formally responded to TSA's public notification of intent to alter record systems in September 2004. According to EPIC, "TSA must take into consideration the privacy interests of those whose information is gathered, and take great care to guard this information from excessive use, misuse, or even use in furtherance of a terrorist act."

TSA maintains the TWIC program fully complies with all federal privacy laws and that all of the information stored within the card is encrypted for added security. In addition, no personal information outside of the holder's name and photo will be visibly displayed on the TWIC, unlike many driver's licenses and other forms of identification that display a social security number or home address.

Status

In April 2003 TSA initiated operational testing by conducting a six-month technology evaluation at 12 different transportation facilities, not all of them maritime. The evaluation successfully demonstrated TSA's ability to open and manage enrollment centers and to produce and issue cards and the TWIC's ability to support physical and logical access control. Most importantly, the evaluation period provided TSA the opportunity to evaluate the feasibility and reliability of existing card-based technologies in the field, including the integrated circuit chip, linear barcode, magnetic stripe, optical memory stripe, and the two-dimensional barcode.

The next phase of testing, protoype, was conducted from August 2004 to June 2005. These tests included use of the TWIC system at selected deepwater ports throughout the country. According to TSA, the prototype successfully tested advanced components of the TWIC, including its ability to manage a centralized and uniform card production system, physical access interfaces, and the operation of a centralized identity management infrastructure. While the actual number of cards used for access control was less than anticipated, the valuable lessons learned regarding the concept were incorporated in the planning stages for implementation.

After missing the initial target date for issuance in August 2004, Congress requested that the Government Accountability Office (GAO) conduct an audit of the TWIC program to identify the cause of the delay and to document future challenges facing timely implementation. In December 2004 the audit was complete and cited three main issues for the delay.

According to the report, the first reason for the delay was that TSA had difficulty in obtaining approval for the prototype test from the Department of Homeland Security. GAO did recognize that DHS was a newly formed agency at the time, with multiple legacy projects and urgent security responsibilities, especially in the aviation arena.

Second, TSA was tasked to work with DHS and Office of Management and Budget (OMB) officials to identify additional information needed for a second cost-benefit analysis and alternatives analysis. This required additional time, further delaying the prototype test.

The third reason cited by GAO for missing the August 2004 deadline was a congressional request to conduct additional tests of various card technologies, which resulted in another seven-month delay to the original testing schedule. Regarding the additional testing, GAO stated: "This analysis is typical of good program management and planning and, while it may have delayed the original schedule, the purpose of such assessments is to prevent delays in the future." The GAO report can be found in its entirety at www.gao.gov/new.items/d05106.pdf.

One Size Does Not Fit All

In developing the TWIC regulations, TSA has employed industry working groups, union representatives, other DHS offices, and internationally recognized standards organizations for assistance. The Coast Guard has also received valuable guidance and support from the National Maritime Security Advisory Committee's Credentialing Workgroup. Both agencies expect considerable feedback and recommendations from industry and labor organizations during the notice of proposed rulemaking comment period that will precede the regulations.

Impact on Merchant Mariners

Depending on their service, U.S. merchant mariners currently must carry a license (or Certificate of Registry, if a staff officer) or a merchant mariner's document (MMD) or both, and, if they sail beyond the boundary line, they must also carry a separate STCW Endorsement. These credentials are referred to generically as merchant mariner credentials (MMC).

As the MTSA requires all individuals holding an MMC to have a TWIC, regardless of a need to access secure areas, the Coast Guard's National Maritime Center has expressed concerns over adding yet another credential to the list of those already required for mariners. To address this issue, the Coast Guard is currently evaluating a draft proposal to combine all MMCs into a single form.

The current proposal would enable mariners to carry no more than two documents, with the TWIC serving as the identity document and the MMC, consisting of a combined license, MMD, and STCW endorsement, serving as the qualification document. Timing such a change to coincide with the TWIC roll-out would simplify the process for the more than 62,000 mariners who would benefit from this consolidation.

Conclusion

A significant contribution the Coast Guard brings to the project is the technical appreciation for the vast differences among the numerous MTSA-regulated facilities, vessels, and outer continental shelf platforms, which are not easily amenable to a uniform application of the TWIC. Also, because Coast Guard is responsible for the security plan approval process for all regulated vessels and facilities, it can assist with the integration of all TWIC requirements and components in the existing security plans. While the task is certainly not an easy one and the regulatory development process has taken much longer than expected, the final product will provide another tool to improve security at U.S. seaports, while enhancing commerce and protecting personal privacy.

About the author: *LCDR Jonathan Maiorine is currently serving as a TWIC project team member for the Coast Guard and is assigned as Chief, Standards Branch for the Coast Guard Office of Port and Facility Activities. He is also overseeing the current update to Title 33, Code of Federal Regulations Subchapter H, Maritime Security Regulations.*

Special thanks to LTJG Nanine Nyman for assisting with the drafting of this article. She is currently serving as both a member of the TWIC project team and biometrics subject mater expert for the Coast Guard's Office of Port and Facility Activities.